> "With one such multi-choice set-top box in their homes, consumers could freely choose to subscribe to any MVPD's system, could freely elect to disconnect that system and switch to another, and could even freely subscribe to more than one MVPD service."[31/]

Viacom elaborated:

> "The dual-module box will be universal, such that it can be used by the subscriber to any MVPD service. In addition to being universal in nature, however, the set-top box of tomorrow should accommodate more than one MVPD simultaneously so that a consumer need not purchase multiple boxes upon the subscription to more than one MVPD."[32/]

In a slight twist on such universality, U.S. Satellite Broadcasting Company, Inc. ("USSB") asserts that the Commission rules "should provide that 'commercial availability' includes DBS receiving equipment that is interoperable to function with all DBS signals from a common orbital location."[33/]

The Coalition agrees with Viacom, USSB, and others[34/] that Congress intended Commission action in this proceeding to take steps toward the sort of worthy goals they describe. Coalition members would be pleased to cooperate in industry-

---

[31/] Viacom Comments at 6.

[32/] Id. at 8.

[33/] USSB Comments at 5-7.

[34/] E.g., Comments of Bell Atlantic and NYNEX at 2-4 (stating that "navigation devices must work with systems in different parts of the country and with different types of systems -- 'portability' and 'interoperability'") (emphasis added); Comments of Pac. Bell at 3 (agreeing "that universal boxes and network interface modules should be commercially available, so long as these items do not include the proprietary smart cards and software").

led projects to achieve these goals. As the Coalition indicated in its Comments, however, it believes that the Commission has a truly urgent task in removing basic obstacles to competitive commercial availability, and that these are the obstacles to national device portability.

Until national device portability can be achieved for all MVPD networks, the Coalition would not urge that the Commission seek to assure interoperability among such networks. The entry into the navigation device market from consumer electronics, computer, and other manufacturers, and from national retailers and direct sellers, in response to system support of true national device portability, will lead to marketplace pressures for interoperability of devices among different MVPD systems. The Coalition does not believe that additional steps will be necessary, either across different types of MVPD systems (e.g., cable to satellite to OVS), or within a class of MVPD systems that already supports national competition from truly independent manufacturers and sellers (e.g., DBS).[35/]

[35/] The argument by Besen & Gale that DBS demonstrates that "portability' is not necessary is actually addressed to this question of interoperability among different nationally portable systems. Impliedly, it demonstrates that national portability is indeed a prerequisite for a successful competitively available system. Besen & Gale, GI Comments App. A at 21.

E. Statutory Reference To Manufacturers and Sellers "Not Affiliated" With An MVPD Operator Was Not Intended To Make Section 629 Devoid Of Meaning and Significance.

In our initial Comments, the Coalition and its members generally agreed that the definition of affiliation should be defined pursuant to Section 3(1) of the Communications Act in terms of a minimum 10% common ownership or control.[36/] As we discuss above, however, the fact that non-affiliation is *necessary* to achieve competitive commercial availability was never intended by the Congress to mean it is *sufficient*.

The ITI/CompTIA Comments state a persuasive case for putting the Section 3 definition of "affiliate" in context with respect to "commercial availability":

> Section 3's definition of "affiliate" is limited to relationships between entities involving ownership or control; it does not encompass other types of relationships, such as exclusive contractual arrangements, that may rise to a level comparable to affiliations involving ownership or control. Thus, under Section 3's definition, CPE could be considered "commercially available" through a source "not affiliated" with an MVPD, for purposes of satisfying Section 629(a), as long as the CPE was available from an entity whose relationship with the MVPD involved neither ownership nor control of one by the other, nor joint ownership or control of both by a third party.
>
> But even where there is no ownership or control between an MVPD and a particular source of CPE, the MVPD could nevertheless effectively exclude or limit CPE competitors from the MVPD's markets through exclusive arrangements between the MVPD and manufacturers, retailers, or other

---

[36/] E.g., Circuit City Comments at 24; Tandy Comments at 5; see also CERC Comments at 33-34.

> sources of CPE. If such arrangements have the effect of inhibiting competition in the provision of CPE, they should be viewed as "affiliations" for the purpose of implementing Section 629(a), notwithstanding the fact that such contractual arrangements do not fall within the scope of the statutory definition of "affiliate."
>
> Finally, to satisfy the commercial availability requirement of Section 629(a), CPE must not only be *sold* by at least one entity that is unaffiliated with an MVPD, but, if an MVPD manufactures its CPE (directly or through an affiliate), the CPE should also be *manufactured* by an unaffiliated entity. Section 629(a) specifically includes manufacturers among the types of unaffiliated sources that should provide CPE. If an MVPD is the sole manufacturer of CPE used with its system (either directly or through an "affiliate"), the mere fact that multiple retailers carry the product would not be sufficient to achieve the pro-competitive objectives of Section 629, since the MVPD would still control the supply of CPE.[37/]

We agree with ITI/CompTIA's analysis. Exclusive manufacturing and sales agency arrangements that effectively inhibit competition in the provision of CPE should be viewed either as "affiliations" or as otherwise noncompliant with "commercial availability" for the purpose of implementing Section 629(a), even if such contractual arrangements do not fall within the literal scope of the existing statutory definition of ownership or control in Section 3(a).[38/]

[37/] ITI/CompTIA Comments at 16-17 (emphasis in original).

[38/] Consider the broader definition of "affiliation through contractual relationships" in the new spectrum auction rules, which provide that "affiliation generally arises where one concern is dependent upon another concern for contracts and business to such a degree that one concern has control, or potential control, of the other concern." 47 C.F.R. § 24.720(l)(9).

F. The Right to Attach Must Be Without Qualification Except To Prevent Harm to the Network.

While many Commenters purport to support a consumer right to attach equipment obtained from retail outlets, some simultaneously insist that system operators must be permitted to establish and enforce their own standards as to what may be attached to their systems.[39/]

We agree that the right to attach must be qualified to ensure that the equipment does not adversely affect the network. To this end, the Coalition and its members previously suggested that Parts 15 and 68 of the Commission regulations or equivalent provisions should apply.[40/] No further qualifications should be tolerated beyond such FCC-defined measures to prevent harm to the network.[41/] If MVPD operators are able to impose additional restrictions on subscribers' right to attach or otherwise link consumer equipment to the network, the right to attach will be meaningless.

[39/] GI Comments at 11-12, 69-73; Scientific-Atlanta Comments at 29; see also NCTA Comments at 4-7.[39/]

[40/] E.g., Circuit City Comments at 23.

[41/] In the absence of a security interface, security concerns essentially would eviscerate the right to attach. Despite the arguments advanced for "embedded" security, no one trusts it enough to allow it in competitively manufactured devices. See discussion in Section II.C. below.

II. THE CASE FOR A STANDARD TO SEPARATE SECURITY CIRCUITRY FROM OTHER FEATURES AND FUNCTIONS IS NEARING CONSENSUS SUPPORT IN CONCERNED INDUSTRIES.

As discussed above, it is fruitless to advocate competitive commercial availability without also advocating some standard, privately or publicly achieved, that will remove the most basic obstacle to achieving it.

A. CERC Comments Demonstrated The Necessity And Feasibility Of Such A Standard.

The Coalition's initial Comments demonstrated that unless the security circuitry can be separated from the rest of a navigation device, there is no chance that such a device could be manufactured and retailed independently of the local MVPD system. Thus, the Coalition Comments reviewed the progress to date, among several industries, in developing feasible security interface standards for both analog and digital devices.[42/]

The Coalition stressed that the Commission, to take meaningful action, can remain in the realm of technologies whose feasibility has already been demonstrated. We are pleased that additional support for this view came from many other commenters and that it reflects an emerging consensus.

[42/] CERC Comments at 17-23.

B. Commenters From All Other Concerned Industries Also Support Achievement of Such An Interface.

Representatives from virtually all interested industries recognize that it is possible to separate security functions from non-security functions, create a standard security interface, and thus offer commercially available navigation devices without compromising network security -- and, more important, that it is desirable to do so. Indeed, a broad cross-industry consensus is fast developing among MVPD network operators, content providers, hardware and software manufacturers, and retailers.[43/] Consider the comments of:

- The cable industry. NCTA agreed that the way to achieve Section 629's dual goals of commercial availability of CPE and prevention of signal theft "is to separate the security from the non-security functions of [digital] CPE used to access the services of MVPDs and to make only the latter 'commercially available'"[44/]

- The telephone industry. GTE said that "[a]n appropriate balance between MVPD system security rights and 'commercial availability' of CPE can be achieved in a digital environment . . . if MVPDs are permitted to provide security equipment on a split basis . . . . This would necessitate the creation of standard security interfaces for

---

[43/] The Coalition recognizes that those adhering to the consensus as to the desirability of separating security from other navigation circuitry may disagree with it on other questions, including how active the Commission should be in assuring that this objective is achieved.

[44/] NCTA Comments at 8, 26-28. See also Time Warner Comments at 11-12, 28, 41 (discussing need to separate security functions from non-security functions in commercially available navigation devices, and to establish a common interface for a renewable and removable security module to be used with digital navigation devices); Comments of U S West at 2-4, 12.

devices to work with multiple service providers. It is both feasible and advisable to have a standard interface."[45/]

- The program provider industry. Viacom promoted standardization of a "universal, multi-choice digital set-top box," with a smart-card based conditional access system, and standardized connection for a separate security device.[46/]

- The consumer electronics industry. CEMA said that "there is no essential technical reason why the security and non-security functions of navigation devices cannot be decoupled."[47/]

- The information technology (computer) industry. ITI/CompTIA said, "In non-competitive multichannel video services markets, safeguards should be designed to prevent the bundling by MVPDs of security devices and non-security devices and/or programming services. . . . The affected industries (including MVPDs and competing CPE manufacturers) should cooperate in the development of interfaces for interconnection of security and non-security CPE."[48/] And, of course,

- The retail industry.[49/]

[45/] GTE Comments at 7. See also Comments of Bell Atlantic and NYNEX at 6; Pac. Bell Comments at 3.

[46/] Viacom Comments at 6-9.

[47/] CEMA Comments at 16. See also Comments of Zenith Electronics Corporation at 13 ("If the Commission is to be successful in truly making set-top devices commercially available, the standardized interface must be a high priority and come to realization before the installed base of digital CPE devices, both set-top boxes and television receivers, grows to a point at which the economics of changing out non-compliant CPE precludes the implementation of the retail model.").

[48/] ITI/CompTIA Comments at 24-25. See also Comments of the Ad Hoc Computer and High-Technology Coalition ("CHTC") at 9-10 (advocating a standard interface for reading digital software carriers in the digital domain).

[49/] Circuit City Comments at 31 (stating that security circuitry should be isolated from all other circuitry so that it can be provided separately and directly by the network operator to the customer, with a common interface for mating such security circuitry to other circuitry); Tandy Comments at 13.

It is, essentially, only those with a direct stake in the noncompetitive *status quo*,[50] and those who would deny MVPD operators the right to exclusive control of security circuitry,[51] who still interpose a blanket objection to the emerging consensus as to separation of security from non-security functions.

C. Arguments for Perpetuating Embedded Security Are Unpersuasive and Contrary to Experience.

Ironically, the commenters who most determinedly do NOT want to see a standard allowing security to be renewable, and always replaceable by the system operator, arrive at this position from different ends of the business spectrum: all of General Instrument's cable customers are cable operators; none of Commercial Engineering's are. Yet they share an antipathy to a national security interface because each does not want to see cable MSOs able to maintain control over security by being able efficiently to replace the security circuitry in case of a breach.[52]

---

[50] GI Comments at 56-61; Scientific-Atlantic Comments at 24-25. However, even Scientific Atlanta observes that in some uses, such as its Pegasus terminal, smart card technology and separating out security can be helpful. Id. at 25.

[51] Comments of Commercial Engineering at 6-7.

[52] GI advocates other approaches to renewability (but not sufficient to support fully independent manufacture and sale of the devices), and acknowledges the right of some MVPD customers to choose to support a security interface. GI Comments at 60. Unless supported by all cable systems, however, such an interface cannot support national portability, so will fail to attract competitive devices.

Commercial Engineering ("CE") opposes a national security interface because it disputes the right of a cable system operator to maintain physical control over the security function.[53/] It argues:

> [Commercial Engineering] strongly disagrees with the concept of separate security components under the control of the cable operator which are distinct from the remainder of the navigation device. CE does not believe that such a "split the baby" type of proposal squarely meets the intent of Congress in insuring consumer availability of navigation devices, of which the security component is an integral and essential part. Likewise, under the type of system envisioned by CE, a consumer should not have to wait on installation of security by way of card, programming, separate module, etc. by the cable provider. This would serve to defeat the intent of the legislation by turning consumers away from commercially available equipment which can only be activated at the whim and convenience of a reluctant cable operator.[54/]

The Coalition disagrees with this notion of competitive availability. Existing state laws and Federal policy cited in the NPRM require that navigation devices should, indeed, be activated only "at the whim" of the cable operator. It is the concern over potential abuse of the system, and loss of revenue for valuable services, that causes those who advocate "embedded" security to mistrust fully competitive manufacture and sale of navigation devices.

The fact that those who oppose operator control also oppose a national renewable security standard underscores an important point: renewable security allows the system

---

[53/] Comments of Commercial Engineering at 6-7.

[54/] Id. at 6.

operator to keep control of security circuitry at all times. Embedded security, by contrast, involves essentially a one-time decision by the device manufacturer, after which the operator loses efficient physical control.

1. Critics of a national security interface confuse experience with existing "smart cards" with a truly renewable interface such as NRSS.

The "smart card" implementations discussed and criticized in the appendices to the General Instrument[55/] and Time Warner[56/] filings differ from both the "A" and "B" versions of National Renewable Security Standard ("NRSS"). In the "smart card" implementations criticized, the circuitry for controlling "conditional access" resides on the card, but the descrambling "decoder" circuitry remains embedded in the host device. While such an implementation supports portability and a degree of renewability, it remains vulnerable to the hazards of embedding security, and it opens an interface, between the two major security elements, that invites attack.

[55/] GI Comments at 58-59; see also, Eric J. Sprunk, Director, Access Control & Security Technology, GI, Smart Card Technology & Broadcast Systems White Paper (Apr. 1, 1997) (attached as Appendix D to GI Comments), and references by Besen & Gale, GI Comments App. A at 10, and 13.

[56/] See Internet Excerpts by John McCormac, Editor, Hack Watch News (attached as Exhibit A to Time Warner Comments). Time Warner bases its criticism of the "A" option of NRSS on these arguments, but supports the NRSS "B" option as the basis for a national standard. Time Warner Comments at 11-12. The Coalition, in its comments, urged that an option choice emerge from the adoption of specific performance requirements by the Commission. CERC Comments at 20 & n.17.

The incorrect criticism of the NRSS "A" option arises from the fact that it uses a "fat" version of the ISO 7816 card that is also employed in existing "smart card" implementations. Unlike those systems, however, NRSS "A" places the descrambler chip on the card as well. Therefore, in both the "A" and "B" options of NRSS, ***every transistor comprising the security circuitry resides on the renewable card.***

As GI admits in discussing its own history with embedded security,[57] flawed implementations of any security system will be subject to assault. Even excellent implementations may be attacked and ultimately defeated. The advantage of a fully renewable security interface is that the system operator can reassert control without the prohibitively expensive task of physically recovering every box.[58] This fact, and the local system variations made possible by the interface, should discourage attacks in the first place.

---

[57] See generally Marc L. Taylor, GI, DigiCipher®II/MPEG-2: Open Standards, Licensing, and Complete System Development (Apr. 1997) (attached as Appendix C to GI Comments).

[58] Even Besen & Gale cite a case of a flawed security implementation that was cured through the distribution of renewable security cards. Besen & Gale, GI Comments App. A at 10. As long as a system maintains boxes with embedded security, this cure is not available.

2. Embedded security systems defeat operator flexibility.

Coalition members, as retailers, have no inherent reason to prefer one mode of security over another. For us the question is: which system will give MVPD operators the confidence and flexibility to support competitive manufacture and sale? Which system will continue to frustrate the ability of operators to support such a model?

Decades of experience have shown that embedding security circuitry in navigation devices denies cable operators the flexibility and confidence necessary to support competitive commercial manufacture and sale. The law's requirement to maintain MVPD system security is not written on a clean slate -- the cable industry, with its security embedded in boxes whose distribution it fully controls, complains that it loses over $5 billion annually to theft of service.[59/] Under such circumstances it can hardly be expected that operators will support the introduction of devices, with embedded security, made and sold by truly independent manufacturers and retailers.

The declaration by the NCTA that cable operators will move to implement a renewable security interface,[60/] and the support by Time Warner for implementation of such an

---

[59/] Time Warner Comments at 24.

[60/] NCTA Comments at 28.

interface as a Commission standard,[61] are made in recognition of the fact that only a renewable security interface allows operators to support competitive commercial availability.

D. Comments Demonstrate That National Portability Through A Security Interface Is Consistent With Preserving Local System Competition and Features.

Several commenters, while supporting national portability and/or interoperability, expressed concern that the look, feel, operation, and other competitive characteristics of local systems be preserved.[62] The Coalition and others have argued that the best way to assure that competitively procured devices will be able to address varying local systems is to require public notification of system functions and features.[63]

---

[61] Timer Warner Comments at 40-41. The Time Warner Comments refer, additionally, to copyright concerns that should be considered with respect to such a standard interface. The Coalition believes that the private sector standards bodies addressing the NRSS and/or host devices can and should deal with such concerns. This task should not be the basis for any Commission delay in adopting or adapting private sector standards.

[62] E.g., Americast Comments at 4-5; NCTA Comments at 29-30; Pac. Bell Comments at 3. See also GTE Comments at 6.

[63] CEMA Comments at 13-14; CERC Comments at 29; Circuit City Comments at 21-22; ITI/CompTIA Comments at 10-12; BSA Comments at 8-9.

1. The Coalition supports the call of NCTA and Time Warner for a common integrated hardware platform that can be conformed to local systems through software.

The comments by NCTA and Time Warner demonstrate that competitive devices can indeed access local systems, while these systems still preserve their unique characteristics. NCTA, in discussing a standard for separating security circuitry from other circuitry, observed:

> [W]hile industry standards-setting bodies will no doubt consider all relevant MVPD concerns in adopting a separations standard, any such standard must ensure that the MVPD can control and pass through any of its services . . . . Therefore, the commercially available CPE must have a common integrated hardware platform to permit MVPDs to download to and execute applications in that CPE to support features and services on a transparent basis.[64/]

Time Warner makes a more explicit proposal along the same lines:

> Once network security components have been removed from the navigation device, what remains are a number of other functions which are necessary for these devices to interface properly with MVPD distribution systems and support the services offered by a particular MVPD such as tuning, demultiplexing, demodulation, decompression, program guides and other on screen display support, and the ability to support impulse pay per view ordering and program delivery. A hardware transparent applications environment which can be accessed and addressed by the MVPD service provider should be part of every commercially available navigation device. The minimum architectural requirements for such a platform could easily be specified. Such standardization would allow a variety of functions to be integrated using a single microchip processor.

[64/] NCTA Comments at 29-30.

* * *

> A common architecture supporting a hardware transparent addressable applications environment must be flexible enough to support a multiplicity of applications, both present and future, obtained from a variety of sources. This would be greatly facilitated through the use of a common executable programming language, such as HTML, compatible across different operating systems. Indeed, a standardized client-server based HTML engine integrated within all digital navigation devices would greatly enhance interoperability and portability of these devices, as well as harmonize the world of the personal computer with the world of the television.[65/]

The Coalition endorses Time Warner's idea as a creative and feasible approach to facilitating competitive manufacture and sale of devices, yet preserving the right of local systems to promote their features and customize their offerings.[66/] Coalition members will be pleased to work pro-actively to achieve these ends in the private sector standards arena, subject to specific performance requirements adopted by the Commission in this proceeding.

2. As progress with cable modems indicates, standards can be a basis for, rather than obstacle to, progress.

NCTA's idea of a common integrated hardware platform, and Time Warner's creative approach to implementation, demonstrate that the right sort of standardization can support, rather than hinder, both technical progress and

---

[65/] Time Warner Comments at 42-43.

[66/] These Comments also serve to assuage the concerns raised, e.g., by Besen & Gale that competitively available devices cannot efficiently be made to address varying local systems. GI Comments App. A at 23-25.

technical freedom. These sort of standards are seldom arrived at too early. For example, the Commission's adoption of the RJ-11 jack, though reluctant,[67] has done everything to promote, and nothing to hinder, CPE portability and interoperability.

As commenters of several shades of opinion note, the cable industry has moved with admirable speed to establish standards that support the competitive commercial availability of cable modems -- despite the fact that the technology involved is far "newer" than those pertaining to the distribution and security of audiovisual signals.[68] This demonstrates that technological novelty need not be a bar to standardization. Indeed, when the standard -- as in the case of a common security interface and a common hardware platform -- provides a basis for future innovation, standardization should occur when, and while, its benefits are recoverable. Once different and inconsistent interfaces and platforms pervade a technology, the real obstacles to progress arise.

E. While The Commission Need Not Create Standards Itself, Prompt Announcement Of Performance Requirements Is Essential.

In light of the good news from the private sector standards front and the enthusiasm for competitive

---

[67] See Circuit City Comments at 7-8.

[68] E.g., GI Comments at 36-37; Scientific Atlanta Comments at 11; Tandy Comments at 11.

commercial availability now being heard from the cable industry, the Commission might be tempted to take a relatively passive role in enforcing Section 629. As the Commission's experience in waiting in vain for a private sector standard RJ-11 telephone jack[69/] indicates, however, action to get "over the hump" may be essential to aligning industry's pent up competitive energies. The Commission cannot afford the risk of passivity; if new digital systems inconsistent with competitive commercial availability are widely installed in the interim, an ultimate, purely private-sector standards solution may no longer be possible.

Most Comments in support of competitive commercial availability urge the Commission to set performance standards, which should demonstrate or compel the necessity of private-sector standards action, rather than set standards itself. The Coalition would not be averse to Commission standards setting, as in the case of the RJ-11 jack, as a last resort. The Comments, however, appear to support the view expressed by the Coalition on May 16, 1997 that sufficiently specific performance standards, according to an aggressive time schedule, will serve to avoid the risk of the Commission missing the standards "window" of opportunity.

[69/] See Circuit City Comments at 7-8.

III. ARGUMENTS FOR COMMISSION INACTION IN THIS PROCEEDING WITH RESPECT TO AN ANALOG SECURITY INTERFACE ARE NOT PERSUASIVE.

There is a lack of specificity, as well as some inconsistency, among the arguments advanced by those commenters who urge the Commission to ignore analog devices and technologies in this proceeding. They argue:

> (1) Analog technology is being phased out anyway; it would be a diversion of resources to try to achieve national portability among analog navigation devices;[70/]
>
> (2) Whereas digital technology lends itself to solving security interface obstacles to national portability, analog technology does not;[71/] and
>
> (3) In another Docket, the Commission has already created an analog security interface, so need not address the subject in this one.[72/]

The Coalition believes that even if point (1), repeated by many commenters, turns out to be true, the absence of an analog security interface may nevertheless be an obstacle to competitive availability of both digital and analog devices well into the future. Points (2) and (3) cannot both be true. Moreover, while the Coalition is indifferent as to in

---

[70/] E.g., GI Comments at 40-41 ("Analog technology is increasingly giving way to digital technology in MVPD systems. The period of this transition is still unknown. It makes little sense for the Commission to undertake the complex task of establishing new rules under Section 629 for analog devices when, in fact, such devices will increasingly be supplanted."); NCTA Comments at 12-13; Pac. Bell Comments at 2; Zenith Comments at 4.

[71/] E.g., NCTA Comments at 8-10; Time-Warner Comments at 34; U S West Comments at 3-4.

[72/] GI Comments at 3-40; NCTA Comments at 11-12. See also Time Warner Comments at 6, 34-35 & n.52.

which docket the Commission solves the obstacle of an analog security interface, the result urged by those who advance both points (2) and (3) seems to be that the Commission should do so in neither. This would be contrary to both the requirements of Section 629 and determinations already made by the Commission in ET Docket 93-7.

A. Hybrid Systems And Devices May Persist Well Into The Future; A Continued Requirement to Embed Analog Security Would Prevent Commercial Availability Of The Digital Navigation Circuitry.

As the Coalition notes near the outset of these Reply Comments, the shift to digital means of transmission will have significant consequences for consumers and industries alike. Even ***if*** strictly digital means of transmission ultimately are employed for broadcast, cable and all other MVPD systems, the 300 million existing analog TVs and VCRs will continue to be viable with a digital-to-analog conversion device.

There is no requirement, however, that every MVPD system switch to 100% digital means of transmission. System operators, to serve those TVs and VCRs for which consumers will not or cannot purchase digital appliances, may persist in offering analog as well as digital channels, subject to analog, as well as digital, security techniques. Allowing the analog security to remain embedded in new converter boxes means that analog converter boxes can never be subject to true competitive availability. Moreover, allowing such

embedding means that ***any hybrid boxes offering both digital and analog functionality could be supplied only by the system operator***, even though a National Renewable Security Standard (NRSS) for digital transmissions may have been fully implemented.

Commenters who have argued that analog cable transmission technology is "old" have not supplied any information as to whether, or when, it will disappear from MVPD systems. Even if such projections were made, there is no requirement that such a phase-out actually occur. Given this circumstance, and the existence already of an analog security interface, it is much more sensible for the Commission to:

> (1) make a finding in this Docket that an analog security interface is necessary to achieve competitive commercial availability of analog and hybrid navigation devices, and
>
> (2) proceed, pursuant to this Docket, Docket 93-7, or both, to require the support of such an interface on a prospective basis.

B. The Commission Has Already Required, And The Private Sector Has Already Designed, An Interface Providing For A Separate Analog Security Module.

As the Coalition noted in its initial Comments, in some respects the issue of achieving an analog security interface is more straightforward for the Commission because it has already ordered the submission of one, and received a draft standard including one, in ET Docket 93-7.[73/] As the

---

[73/] CERC Comments at 20-22.

Coalition has demonstrated repeatedly, to the extent such an interface is necessary to achieve competitive commercial availability, no other provision of law can or should discourage the Commission from overseeing its implementation in navigation devices.[74/]

1. The fact that an analog security interface has already been developed in another proceeding argues in favor of, rather than against, its implementation in navigation devices.

Some commenters who urge the Commission to do nothing in this proceeding with respect to an analog interface argue that the issue is "settled" in ET Docket 93-7.[75/] If so, where in commerce are the security modules envisioned there? Where are the devices designed to accept them? Clearly, work on this subject remains to be done.

Coalition members are indifferent as to which "FCC" -- the 93-7 Commission or the 97-80 Commission -- oversees the analog security interface. We are concerned, however, that unrelated issues of system automation and communication may be seized upon, in the context of ET Docket 93-7, to bar successful completion of the need identified in this proceeding. This would be contrary to the explicit intention of the congressional committee that wrote both of

---

[74/] Id. at 22 n.20.

[75/] GI Comments at 39-40; NCTA Comments at 11-12.

the Telecommunications Act of 1996 ("1996 Telecomm. Act") provisions that impact on this question.[76/]

What is required, then, to assure the implementation in navigation devices of the analog security interface that has already been designed, or some equivalent interface, is a clear finding in this proceeding of the necessity of such an interface to enable competitive commercial availability of navigation devices on a prospective basis. For those systems not making use of interdiction or broadband descrambling, this is the only way to achieve such availability.

2. Nothing in Section 629 conceivably supports the idea that the issue of an analog security interface has been settled through a "prior determination."

GI argues that the Commission's previous decisions in ET Docket 93-7 with respect to the Decoder Interface and consumer ownership of analog descramblers constitute "prior determinations" under Section 629(d)(1) which "shall fulfill the requirements of [Section 629]"; therefore, analog equipment is exempted from Section 629.[77/] This argument fails on both the facts and the law.

First, unfortunately, ET Docket 93-7 is far from complete. A motion for reconsideration is pending; GI itself has moved for "clarification" on the very issue of

---

[76/] See CERC Comments at 22 n.20 and Section V.A. hereinbelow.

[77/] GI Comments at 39-41.

the security interface, and the issue of applying the analog security interface to all navigation devices (not just "set-back boxes") has been reserved by the Commission for a future determination.[78/] Nor is the Commission's determination in ET Docket 93-7 that it will not require the competitive commercial availability of converters with embedded security of any consequence to the Coalition, as we have agreed that the vulnerability of embedded security should preclude such a measure.

Second, the statutory language cited by GI was added to address concerns raised in the private sector that the "sunset" provision of section 629 arguably could be cited as a basis for re-opening, and then sunsetting, previous Commission determinations with respect to the *unbundling* of telephone CPE. It was never intended to, and does not, address products that have not yet been made commercially available.

C. Commission Regulations, Whether Promulgated In This Docket Or In Docket 93-7, Should Require Use and Support Of The Analog Security Interface On A Prospective Basis.

The arguments against applying the Commission's mandate in this proceeding to analog devices stem in part from a misunderstanding as to what is being proposed. This

---

[78/] See generally Memorandum Opinion and Order, In the Matter of Implementation of Section 17 of the Cable TV Consumer Protection and Competition Act of 1992: Compatibility Between Cable Systems and Consumer Electronics Equipment, ET Docket No. 93-7, 11 F.C.C. Rec. 4121, at ¶¶ 30-39 (1996).

Coalition, at least, does not propose that the analog converter boxes currently in use, which employ embedded security circuitry, should be required to be put in retail distribution or made subject to independent manufacture. The Coalition supports the right of the MVPD operator to have more effective control of security circuitry.

However, the impediment of embedded security ought not to be a key to monopoly on a prospective basis. As the Coalition argued in its comments, after a date certain the support in systems of an analog security interface, and the provision of security modules designed to such a standard, should be required.[79/] MVPD operators should be allowed to retain those analog converters presently in distribution over a phase-out period that comports with their remaining useful life. Newly manufactured analog devices placed in service, either by the system operator or competitively, should support the security interface.

IV. COMMISSION REGULATIONS SHOULD REQUIRE USE OF THE APPROPRIATE SECURITY INTERFACE, ON A PROSPECTIVE BASIS, WHENEVER THE MVPD SUBJECT TO SUCH REGULATIONS FURNISHES SECURITY CIRCUITRY.

Several commenters argue that, even after national security interfaces are achieved, system operators should be able to continue to distribute navigation devices in formats unavailable to commercial competitors (e.g., devices with

---

[79/] CERC Comments at 23.